ARIZONA ELECTRONIC RECORDKEEPING SYSTEMS (ERS) GUIDELINES[1]

Draft 2.0 : 21 June 2002[2]

> *Have you noticed that the word* document *doesn't mean much these days? It covers everything from a text-only wordprocessing file to a spreadsheet to a Java-soaked interactive Web-page. . . . It didn't used to be like this. A document was a piece of paper – such as a will or passport – with an official role in our legal system. . . . The fact that we can't even say what a document is anymore indicates the profundity of the change we are undergoing in how we interact with information and, ultimately, our world.*[3]

The Arizona ERS Guidelines are designed to ensure that information in electronic information systems meets legal requirements for recordkeeping and is acceptable as evidence. These requirements must be addressed in any recordkeeping system, whether fully automated, manual, or a hybrid.

These guidelines represent a consensus among several communities with overlapping interests in electronic recordkeeping, including information technologists, records managers, and archivists. They attempt to focus on business processes, rather than on records or technology. They do not reflect a particular discipline's or agency's perspective. Because the guidelines include only general recordkeeping requirements, an agency must also consider requirements specific to its business processes imposed by law or industry standards.

BACKGROUND[4]

E-Government and E-Records[5]

Computers and related technology have afforded government tremendous new powers to generate, store, distribute and manage vast amounts of information. Information that was once recorded on paper is now kept in electronic systems.

Changes in workflow and business processes, coupled with fundamental differences between information in paper and electronic formats, have clouded many individuals' understanding of what a record is and what records they must keep. Records managers, archivists, and system designers have come to realize that paper records' physical form captures important information necessary to ensure the authenticity and reliability of the record.

In order to ensure that e-records are authenticity and reliable, an ERS must not only include the same information (content) in a paper recordkeeping system, but must also capture information about the records' context and structure that is inherent in the physical characteristics of a paper-based system.

› Content is the substance of a record – the text, data, symbols, numerals, images, sound and vision – that captures sufficient information to provide evidence of a business transaction.[6]

---

1 The Arizona ERS Framework is based on the National Electronic Commerce Coordinating Committee's (NECCC) *Electronic Records Management Guidelines for State Governments*. The Arizona Framework also draws on the Delaware Public Archives' *Model Guidelines for Electronic Recordkeeping Systems*. References to these documents are made in endnotes, represented in the text by superscript miniscules.

2 This draft reflects comments made at the 14 May 2002 Framework meeting. A few sections of this draft highlighted in yellow are still under development; text represents key concepts, but are not yet developed.

3 David Weinberger, "What's a Document?," *Wired*, August 1996, p. 112. Cited in David M. Levy, *Scrolling Forward: Making Sense of Documents in a Digital Age* (New York: Arcade, 2001), p. 21.

4 The general background will almost certainly be split into another document in the next draft.

5 Thanks to Rich Dymalski for his assistance with this section.

- Context refers to the business and technical environment in which a record is created. Contextual information is often extrinsic to the record itself; in a paper record, this information may be captured through physical location (custody) or through policies or procedures that dictate how the record is handled. Context indicates who, what, why, where, when, and how a document came to be.

- Structure includes the internal organization of the formal elements of the record's content, as well as the record's associations and relationships to other documents. Structure may include information about fonts; line, paragraph, and page breaks, and or about other editorial devices that affect the understanding of the document. For example, the space visually defines the elements of a table gives meaning to the contents of those elements. External structure may associate an individual record with other records in the same series, in the same dossier, or to other members of a compound document.

The context and structure of paper records is inherent in physical characteristics of a paper document (including its arrangement within a larger collection of records). For electronic records, a significant portion of the context and structure of the record may be embedded in software and hardware, external to the record and easily dissociated from the record.[7]

With electronic records, the process of creating and managing records is much more important than the format, media, software, or hardware used to create or store the records.[a] An ERS must include the functionality to ensure that the content, context, and structure of records sufficiently document the business process and demonstrate the records' authenticity and reliability.

Unless an electronic system respects the particular requirements of recordkeeping, the information it contains may not be accepted as evidence on the grounds that it is not reliable, is not authentic, or has been altered. Without authentic, reliable, and legally acceptable e-records, e-government may falter or fail. Incorporating sound electronic records management principles in an ERS will ensure that the public, corporations, and others doing e-business with the government can have confidence that the resulting e-records are trustworthy.

ERS Functionality Should be Based on the Value of Records[b]

Addressing the challenges of electronic records requires appropriate resources, and an ideal system may be quite expensive. The effort and expense necessary to design an ERS should balance the value of the records against the potential benefits and costs of automation. The State Library and Archives Records Management Division works with agencies to appraise their records and establish appropriate retention periods for those records.

Level of Risk Exposure

Just as with paper records, the e-records an agency produces or receives are not all of equal importance or value. For example, it makes little sense to invest large sums of money in a system that contains records that are of transitory value and pose little risk of litigation. While an ideal ERS offers many possible recordkeeping features, an ERS should not attempt to implement a higher standard of

---

6 "[Content] encompasses the complete set of documentation required to provide evidence of a business transaction," Center for Technology in Government, State University of New York at Albany. *Practical Tools for Electronic Records Management and Preservation* (Albany: the Center, 1999).

7 The separation of content from contextual and structural information in automated systems is reflected in the 1997 Federal District court decision in Public Citizen v. John Carlin (2 F. Suppl. 2d 1 (D.D.C. 1997)) which notes that an electronic message is not necessarily equivalent to its printout. "[The] difference between electronic and paper records illustrate the fact that the administrative, legal, research, and historical value of electronic records is not always fully captured – indeed, is usually not captured – by paper or microfiche copies. Electronic records therefore do not become valueless duplicates or lose their character as 'program records' once they have been printed on paper; rather, they retain features unique to their medium."

recordkeeping practices than is appropriate to a trustworthy manual (paper-based) recordkeeping system unless there is a clearly demonstrated benefit or business need.

All government records should be well managed to ensure that they are preserved, accessible, and disposed of properly. However, the effort and resources a state agency expends to manage records, including e-records, should be related to the level of risk associated with the information contained in the records. Recordkeeping systems containing high-risk records will need greater controls (with a greater expense) to ensure reliability and trustworthiness than would a system containing low exposure records.

Risk management requires an analysis of risks, relative to potential benefits; consideration of alternative measures to address risks; and implementation of the measures that best address risk based on this analysis. In applying risk management to e-records, the following questions should be asked.

- What would be the impact on agency operations if the records were lost or otherwise unavailable?
- Would the agency or others suffer a financial loss if the records were unavailable?
- What is the likelihood that the records would be subject to or needed for a legal action?
- Would the inability to produce the records in a form admissible in court have a critical impact on the outcome of a case?

For more information on risk management, see

- NIST *Risk Management Guide for Information Technology Systems* 800-30 (January 2002, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf).

Business and Administrative Value

Records' primary value results from their ability to help the agency support its ongoing, day-to-day administrative affairs, document legal obligations and to protect legal rights, and to establish fiscal responsibility and accountability. An agency should ensure that the costs of implementing and managing an ERS are commensurate with the value of those records.

The primary value of records almost always diminishes over time. When records are no longer of value to the agency, they should be disposed of by destruction or by transfer to the State Archives.

Archival Value

A small percentage of records have enduring value that warrants the expense of long-term preservation. More often than not, archival records are valuable for their secondary value, information useful to someone other than the agency which created them.

The Arizona State Archives identifies, collects, preserves, and provides access to records in all formats of Arizona state and local governments and of public officials and other individuals. Archival records remain useful for the Legislature, state agencies, and the general public because those records make government accountable to its citizens; provide evidence about public policies and programs; and protect or verify individuals' rights and entitlements. Archival records provide information about the important people, issues, places, and events that make up the story of Arizona's history.

The State Archives has published a more complete description of the appraisal criteria it uses to determine if records are permanently valuable.

For more information on archival value, see *Appraisal Criteria for Archival Records* (Appendix A).

Benefits of an ERS[c]

Records are the corporate memory that capture an agency's information assets. Often they have been painstakingly assembled at great cost. Good recordkeeping is the basis of knowledge management, allowing an agency to make the most of its intellectual capital and operate more efficiently by ensuring that

- Users can find information quickly, increasing the quality of customer service.
- Management decisions are based on complete and accurate information.
- Resources are not wasted, saving resources spent collecting the same information multiple times.
- The costs of storing and preserving records is minimized by destruction of obsolete records.
- The costs of migrating to a new software or hardware platform are minimized by incorporating the migration process into system design.
- The costs of producing all relevant records during discovery is minimized. Discovery orders require that all relevant documents be produced. Developing a classification scheme to indicate where potentially relevant records are stored and disposing of obsolete records (especially copies on backup tapes) to reduce the volume of records that must be searched can save significant time and money during searches. Potentially more important, it minimizes the risk that the Court will discover additional, relevant records at a later date, damaging the agency's credibility.

The use of technology to automate recordkeeping can offer significant savings in staff resources; fewer people are required for filing and retrieving information. Work can be much more efficient; less time is necessary to access information and many people can work in the files simultaneously. E-records require significantly less office space for storage. Quick, inexpensive duplication of e-records makes off-site records storage practical, offering significant protection against disaster.

At the same time, hardware, software, support personnel, maintenance costs, and system migration can quickly counter cost savings.

Finally, the tragedy of the September 11 attacks demonstrated an important benefit of e-records over paper records. Because e-records can be duplicated easily and at relatively little cost, it is practical to keep a backup of all the records at a secure site. Many companies were able to open for business the next day because a copy of their records survived.

The State Library and Archives strongly supports the well-managed use of electronic records as one of the most effective measures an agency can take to ensure business continuity and disaster recovery.[8]

RESPONSIBILITIES FOR RECORDKEEPING

The Role of State Agencies

Every agency must create sufficient records to document its work based on a number of factors, balancing the value of the information, the risks associated with disposal of the information, and resources necessary to capture and maintain the records over time. Once an agency has established the records necessary to be created, Arizona statute requires the agency to establish and maintain an active, continuing program for the economical and efficient management of its public records (ARS §41-1346).

Each agency must designate an individual to manage its records. In particular, staff members should be assigned responsibility for managing the electronic record keeping system and provide evidence of their assignments through position descriptions, administrative memoranda, or other transmitted means.[d]

The Arizona State Library and Archives' Regulatory Role

The State Library and Archives is mandated to oversee the management of public records throughout state and local government in Arizona (ARS §41-1345). The Library and Archives accomplishes its mandate through its Records Management Division by issuing regulations, policies, and procedures, and by publishing guidelines and standards that establish acceptable practice for government agencies. The Records Management Division offers workshops and consults with government agencies to ensure that

[8] ARS §41-1345 requires that agencies implement an essential records program.

the agencies have an effective and efficient records management program in place. The Records Management Division also operates a center for storing inactive records pending disposal. The Library and Archives established the Arizona 'Lectronic Records Taskforce (ALERT) to coordinate e-records activities in state and local government.

Other Agencies' Roles

A number of state agencies have an oversight and regulatory role in recordkeeping.

- Department of Administration, State Procurement Office. Concerned that purchase of recordkeeping systems is cost effective.
- Auditor General. Relies on records to ensure that the agencies are fulfilling their mandate effectively, using resources wisely, and complying with the law.
- Government Information Technology Agency. Implements technical standards to support recordkeeping requirements in ERS, including the ability for different agencies to share data between systems. Requires a project investment justification if an electronic recordkeeping system costs more than $25,000.
- Secretary of State's Office. Oversees compliance with electronic signatures regulations.

Because these agencies have overlapping interests in electronic recordkeeping systems, they are important partners in the Arizona 'Lectronic Records Taskforce (ALERT).

REQUIREMENTS FOR RECORDKEEPING

General Requirements for Recordkeeping

Recordkeeping is one of the most basic functions of government agencies. People rely on government to maintain social order by tracking important public information, ranging from birth and death certificates to property records. Records track the government's activities, ranging from tax collection to development of major programs through legislation.

In a democracy, access to records enables the public to hold government officials and employees accountable. The information contained in government records documents past and current actions, decisions, procedures, and policies, and may reveal unacceptable inefficiencies or a failure to follow procedure. The failure to create or the destruction of records opens government to accusations of fraud, impropriety, or political embarrassment.[9]

The following two paragraphs need to be blended.

An underlying principle of democratic government is that public records are the people's records, and the officials hold the records are merely trustees for the people. As trustee of the people's records, government is responsible for

- maintaining, protecting, and preserving the information entrusted to it;
- assuring prompt access to the information,
- securing the confidentiality of the information that is not subject to disclosure,
- insuring the content and context of the original information is not compromised,
- providing verification that the originator of the information is still secure and valid.

An agency's implementation of and ERS should continue to uphold the people's trust by establishing policies and procedures to address the access, security and retention requirements associated with

[9] See Kansas Electronic Records Management Guidelines, http://www.kshs.org/archives/ermguide.htm#2.

information derived and transmitted from its recordkeeping systems. An agency must establish controls and practices to ensure that its information is accessible and secure. The integrity, availability, recoverability, and appropriate use of all information assets must be ensured throughout the processing of that information.

All Arizona agencies are required by law to have a records management program in place to accomplish these goals.[10] Records management systematically links business processes to records – in paper or electronic format – in order to

- Capture or create (record) the information necessary to support and document the process.
- Ensure that the records are accessible (can be located) as long as they are needed.
- Retain records as long as they are needed to support the entire process (including reference after the transaction which generated the record is completed). In some instances, this period is defined by law.
- Ensure that the records are protected from unauthorized alteration or loss.
- Dispose of records properly, either by destruction or transfer to an archives.
- Balance the costs of records programs against the value of the information to the organization.

Systems designers and records managers should work together to design an ERS to properly manage the records it contains. Key factors to consider when developing an ERS include

- Manual recordkeeping systems are often imperfect. When automating an existing system, all business processes that cause records to be created, retrieved, preserved, or disposed should be carefully examined and re-engineered when necessary, rather than merely automating the existing paper recordkeeping system.
- Including records management functions during the development of an ERS makes it significantly easier and less expensive to properly manage the records in the system because the system designers are familiar with the record structure, storage facilities, and processes. Adding records management functions to the software at a later date may be particularly difficult and expensive – and occasionally impossible – because adequate documentation is often missing.[11]
- Special care must be taken to ensure that people have the same trust in e-records that they have in paper records. For example, it is essential that e-records be accepted as evidence in courts. the familiarity of paper records, as well as assumptions, practices, and laws relating to records that give people confidence in paper records do not readily translate into the digital environment.
- The nature of automated record systems introduces new problems that must be addressed. Because people are familiar with paper records, they often have an unconscious ability to verify records. Even individuals with an untrained eye may spot odd paper or ink; irregular or missing signatures or dates; or erasures and may question a record that 'doesn't look quite right.' Because e-records are easier to change, and because those changes do not leave readily apparent clues, an ERS must include the ability to detect unauthorized changes.

---

[10] Records management includes the creation and implementation of systematic controls for records and information activities from the point where they are created or received through final disposition or archival retention, including distribution, use, storage, retrieval, protection and preservation (ARS §41-1346D).

[11] "For conversions to be successful, those performing the transition must have knowledge of the original application and data formats, and the more complex the file structure, the more important this knowledge is. Whether the application is commercial or generated in house, over time this knowledge may be lost and with it the ability to perform a successful migration." United States General Accounting Office, *Information Management: Challenges in Managing and Preserving Electronic Records* (Washington, DC: the Office, 2002), p. 47).

Requirements for Authenticity, Reliability, and Immutability[e]

One of the most important features of records is that they are trustworthy. Records are expected to be consistent over time, that they have not changed or become corrupt and that the information they contain and preserve is authentic (accurate, verifiable) and acceptable as evidence. An ERS can be made untrustworthy if data entry is sloppy, or if users grant unauthorized access as a result of social engineering by a hacker.

Trustworthiness is assessed in terms of a record's authenticity and reliability. All three terms are slippery because they are interrelated and because they are often used interchangeably.[12] Underlying all three concepts is the notion of genuineness, legitimacy, and correctness (veracity).[13] This document will use the following definitions for authenticity, reliability, and trustworthiness.

- An authentic record is what it purports to be. The claims (statements of fact) made in a document can be verified as true. A signature that identifies the creator of a document can be tested to verify that the individual represented by the signature did, in fact, write the document. A document's date can be tested to verify that it was not falsified.[14]
- A reliable record accurately describes the facts as understood at the time of creation[15] and has not been altered to change that understanding.[16]
- A trustworthy system is capable of producing authentic, reliable records.

In order to protect the authenticity and reliability of records, an ERS must address a variety of factors relating to the recordkeeping process, rather than as characteristics inherent in the record itself.[f]

Because it will be necessary to have hybrid paper, e-record systems for the foreseeable future, an agency must establish business rules for establishing the authentic copy of a record if there is a discrepancy between the paper and electronic versions of a record. Those processes must be based on established policies and procedures that will stand up to an audit.[g]

---

12 "Practitioners' understanding and usage of the concept of 'authenticity' and associated concepts are closely related to their working practice and the context of their work experience. Records users and practitioners deal with records every day in their work processes, where they judge the authenticity of records as needed. Through those processes, practitioners have come to create and understand a working concept of authenticity in their own minds. . . . The language used by practitioners to express issues of authenticity differs significantly from the language used by the most prominent research projects." Eun G. Park, "Understanding 'Authenticity' in Records and Information Management: Analyzing Practitioner Constructs," *American Archivist* 64:2 (Fall/Winter 2001), p. 288.

13 "Archbishop Trench, in a series of lectures published in 1882, points to an essential distinction: ' Caesar's The History of the Alexandrian War is not genuine since Caesar did not write it; yet it is authentic in the its contents are accurate and verifiable. Thiers' History of the French Empire is genuinely his work but unauthentic in its content. And Thucydides' History of the Peloponnesian War is both genuine and accurate." John Ciardi, *A Browser's Dictionary* (New York: Harper & Row, 1980), p. 13.

14 "Validating authenticity entails verifying claims that are associated with an object – in effect, verifying that an object is indeed what it claims to be, or what it is claimed to be (by external metadata)." . . . "It is important to note that tests of authenticity deal only with specific claims (for example, 'did X author this document?') and not with open-ended inquiry ('Who wrote it?'). Validating the authenticity of an object is more limited than is an open-ended inquiry into its nature and provenance." From Clifford Lynch, "Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust," *Authenticity in a Digital Environment* (Washington, D.C.: Council on Library and Information Resources, 2000), p. 5-6. Available at http://www.clir.org/pubs/reports/pub92/contents.html.

15 "A reliable record is one that is capable of standing for the facts to which it attests. Reliability thus refers to the truth-value of the record as a statement of facts and it is assessed in relation to the proximity of the observer and recorder to the facts recorded." From Heather MacNeil, "Trusting Records in a Postmodern World," *Archivaria* 51 (Spring 2001), p. 39.

16 Note: Corrections to a record made according to established procedure and with proper authority do not affect reliability.

Deviations from established policies and procedures should raise flags about the authenticity and reliability of the records. Hence, it should be difficult – if not impossible – to circumvent those policies and procedures. The ERS should be part of a larger records management program that includes audits to verify that policies and procedures are followed and that include problem reporting and resolution procedures.[h]

An ERS must capture sufficient contextual information to supplant physical characteristics of manual systems used to authenticate records. The authenticity of paper records is often questioned because of differences in the appearance of a records; the questioned record may differ from other records in the series in terms of paper, ink, handwriting or printing. Paper records may be subjected to forensic analysis to authenticate a document; a record supposedly written in the 1940s using an ink that dates from the 1980s is clearly not authentic.[17] For best practices, see Minnesota's Trustworthy Information Systems Handbook.

General security requirements in support of authenticity, reliability, etc.

General Legal Requirements[i]

Arizona law requires all agencies to "Make and maintain records containing adequate and proper documentation of the organization, functions, policies, decisions, procedures and essential transactions of the agency designed to furnish information to protect the rights of the state and of persons directly affected by the agency's activities" (ARS §41-1346). Federal or state laws may require specific agencies to keep certain records or to keep records in certain formats. When designing an ERS, the agency should consult with legal counsel to determine legal requirements for recordkeeping.

Agencies are required by law to make virtually all records available to the public (ARS §39-121). At the same time, some information in records must be redacted to protect confidentiality or privacy. During the design process, an agency should establish policies and procedures for providing the public with the records and ancillary information contained in an ERS while filtering any information that should be restricted.

For more information on legal requirements for recordkeeping, including a list of Arizona statutes restricting access to records, see [to be modeled after Pittsburgh Warrant Project, Delaware Guidelines].

Information on legal requirements of evidence. (See Federal Rules of Evidence Article VIII. Historical Notes and Commentary. See especially Rule 902.) Ability to produce all relevant documents, including those on backup tapes. In some instances, e-media may be subject to forensics searches that could potentially recover deleted or erased files. Some systems keep transitory copies (in temp files) that most users are unaware of, but which may capture relevant evidence. E.g., Oliver North believed he was deleting email, without realizing that it was kept on backup tapes.

Often, the law defines the contents of specific records that must be kept.

General Business Requirements[j]

Agencies create and preserve transactional and informational records[18] in order to fulfill their mandate. Arizona law requires "all officers and public bodies to maintain records . . . reasonably necessary to

[17] Many ink manufacturers include chemical tags that can be used to test dates. The example is based on a set of diaries attributed to Hitler offered for sale in the 1980s.

[18] The legal definition of a public record in Arizona is particularly broad, including virtually all information that is created or received in an agency that is useful enough to be kept for a period of time. In some instances, that information is in the form of a transactional record that documents a routine business procedure. In other cases, the records contain non-routine reports, spreadsheets, and correspondence.

provide an accurate accounting of their official activities and of any government-funded activities" (ARS §39-121.01(B)).

When designing an ERS, the agency must clearly define the records created by the business process being automated by establishing

- The content necessary for a sufficient record. Typically, the content may include a date, and the names and signatures of parties and witnesses, in addition to the substance of the record.
- When information should be transformed from draft information to a formal record. Creating a static snapshot of information at a moment in time that encapsulates the content, content, and structure of the record is especially important for documents that are created using databases, spreadsheets, or other tools that are not designed to preserve previous versions and are likely to be overwritten.
- The necessary structure of the record, including acceptable variation in presentation formats due to changes in technology.
- Contextual information about the execution of the record to demonstrate that the record is trustworthy and to support the evidential value of the record.
- Sufficient audit trails to demonstrate program accountability.
- That any financial functions conform to generally accepted accounting principles.

Other Administrative Considerations [was: Assumptions about E-Records Environment in Arizona]

An ERS must work within the current economic and governmental environment to balance a variety of legal, business, and technical requirements. When designing an ERS, the agency must work carefully with the system designer to achieve a fundamental goal of records management: to ensure that the costs of incorporating these requirements into the system are justified by the value of the records.

In order to help systems designers balance costs and benefits, the Library and Archives has posed certain assumptions about the current state of ERS in Arizona. The following assumptions reflect the current environment and are subject to revision as that environment changes.

- Manual and electronic recordkeeping systems will exist side by side for the foreseeable future. Manual systems may need to be modified and ERS must be designed so that the two systems are well coordinated.
- ERS are relatively new. A lack of consensus on best practices places any information kept in an ERS at some risk of loss. That risk can be mitigated with good planning and – given the benefits of the ERS – may be entirely acceptable for many records. In general, risk increases with the length of time records must be retained. Agencies should proceed with caution when dealing with records that must be kept for more than ten years and, depending on the level of risk, consider backing up the records in a stable format such as computer output microfilm.
- Few agencies will have additional money for targeted e-records efforts. They will have to pull a percentage of resources from existing activities; some activities may be discontinued, while others may be scaled back.
- The State Library and Archives has redirected funds to help agencies develop policies and procedures to develop strong e-records management programs. However, the Library and Archives cannot implement an e-records management center in the foreseeable future to support custody of other agencies' non-permanent records in electronic format. Agencies will have to bear the costs of managing their e-records – current and inactive – throughout the records' lifecycle, which includes the costs to migrate to new ERS software/hardware or to a non-electronic format.
- Archival information – the three to five percent of permanently valuable information – may be lost if agencies store that information exclusively in e-formats before standards and practices for

permanent preservation of e-records are well established. Until best practices are established, archival information should not be kept exclusively in electronic format.

› People are at the heart of any recordkeeping system, paper or electronic. Because records management requires people to follow policies and procedures, the quality of recordkeeping is human and imperfect. The quality of records management will vary from agency to agency. When agencies have a strong business need for good records, they will invest necessary resources to ensure good records management.[19]

Human Factors

Recordkeeping has always been dependent on human behavior, and that behavior is often imperfect. The mechanical nature of computing allows an ERS to be designed in such a way that it compensates for some of those imperfections. An ERS can greatly increase records' reliability by including automated error checking to validate data and ensure that records are complete.

Systems designers must remember that users – both those who enter data, as well as those who retrieve it – are ultimately the heart of the system. If the system is difficult to use or difficult to understand, users may circumvent the process, making the ERS less reliable because information is missing or inaccurate. Such work-arounds often are not an attempt at fraud, but an attempt to enter information through a 'back door' to get the correct result if they cannot enter it through the 'front door.' Or, users may track information on paper outside the system; although they may intend to enter the information later, date and time stamps will be inaccurate and often the information is never entered.

Training is a significant component to compensate for human factors. Training should include information about the general recordkeeping requirements described above, as well as the use of a specific ERS.[k]

For more information on human factors, see Jakob Nielsen's *Human Factors Engineering* and his Web site at http://www.useit.com/.

Need to emphasize that users are *average*. Cannot make assumptions that rely on users understand technology (operating system or software packages) or that they will behave in a certain way. Variety of factors: respect for process, technological competence, understanding of the system.

FUNCTIONAL REQUIREMENTS FOR RECORDKEEPING SYSTEMS

An ERS must be able to receive, capture, or create records. It must be able to provide selective access to the records and ancillary information in the system based on a user's rights to data. It must be able to maintain and preserve those records over time. Finally, it must be able to dispose of records, either by deleting records from the system or by transferring them in an acceptable format to the State Archives for permanent preservation.

The following sections detail specific ERS requirements in terms of records origin, access, preservation, and disposal. The requirements are stated in terms of general principles, with pointers to guidelines for best practices and supporting technical standards.

[19] Although not a direct study of Arizona's recordkeeping practices, the National Archives and Records Administration's *Report of Current Recordkeeping Practices within the Federal Government* likely translates closely to Arizona's recordkeeping environment. The authors note, "The quality and success of recordkeeping varies considerably across the agencies studied . . . . When agencies have a strong 'business' need for good [recordkeeping], such as the threat of litigation or an agency mission that revolves around maintaining 'case' files, then [recordkeeping] practices tend to be relatively strong *with regard to the records involved*.' [Emphasis in original.] (p. 5)

System Administration Requirements

- An agency must accurately document the ERS system performance and keep such documentation current.[l] Such documentation should
  - Assign system management roles and responsibilities.
  - Define the roles and responsibilities of the individuals involved in the creation, maintenance, and destruction of the records.
  - Provide for consistent quality control, problem resolution, and other activities that might be subject to inconsistent action or misinterpretation.[m]
- An agency should routinely test an ERS to ensure the reliability of the software and hardware.[n] The audit should address the quality of data when entered, security of access, etc.[o]
- Ensure that users are well trained.[p]

Origin/Creation Requirements

An ERS must be able to capture the information necessary to adequately document business processes. It must include sufficient information about the context and structure of the record in order to ensure that the records are acceptable as evidence.

Specific requirements include

- Documented procedures for the receipt, creation, processing, and filing of e-records.[q] These policies and procedures should indicate required administrative, contextual, structural, and preservation metadata; acceptable formats; the conditions that must be met to ensure that the creation or transmission is complete and that the record has been stored in an immutable form.

  Policies and procedures should include routine checks on quality control and mechanism for addressing quality problems. Date entry routines should validate data.

- Create or capture a record for each business transaction.[r] The record must include sufficient content to meet business and legal needs. The record must include adequate information about the record's context and structure, and may include the following elements (which may be system supplied).[20]

  1. *Chronological date*.[s] Must include the time of transmission (to an internal and/or external addressee) and time of receipt.
  2. *Topical date*. The mention of the place where the document is made and/or from where it is transmitted
  3. *Entitling*. Originating address.
  4. *Attestation*. Name or signature of author/writer. If security is such that nobody other than the electronic address holder, that is, the originator, can have access to that address for sending messages, then the entitling does acquire a superscription function, but never an attestation function.
  5. *Inscription*. The name of all addressees and must be distinguished from receivers. While the names of the addressees need to be in the body of the record, that is, constitute an intrinsic element of form, the names of the receivers can simply be linked to the record and constitute an extrinsic element of form, which would fall into the category "annotations".
  6. *Receivers*. Name of copied persons.
  7. *Title or subject*. The identification of content, including the date of the event, fact, or act represented, if different from the date of the record. While traditional non-textual records do not always have a title or subject, non-textual records in electronic form, just like the textual ones,

[20] See InterPARES UBC Project, "Rules for Activities Involved in Manage Archival Framework." Available online at http://www.interpares.org/UBCProject/tem6.htm.

always include a one line title (which is usually called "file name") that is often the subject of the record. This is not sufficient for either textual or non-textual records.

8. *Disposition*. A message expressive of the will or judgment of the author.
9. *Unique identify each record.*[t]
10. *Special sign*. E.g., a digital signature to ensure authenticity.
11. *File details*. File size and format.

Reconcile with Minnesota metadata. Better definition of metadata.

› All records created by the system must be listed on the agency's records retention schedule.[u]

› Designate a receiving device.[v] A specific server or a specific email address or Web site to which records may be addressed. This needs clarification.

› Receipt should be confirmed.[w]

For information on additional schemes to capture administrative, structural, preservation, and other metadata, see

› *Data Dictionary - Technical Metadata for Digital Still Images:* NISO Z39.87-2002, AIIM 20-2002. Draft available for review from 1 July 2002 through 31 December 2003 at http://www.niso.org/standards/resources/Z39_87_trial_use.pdf.

› Minnesota Recordkeeping Metadata Standard (IRM 20), available at http://www.mnhs.org/preserve/records/metamrms.html

Ensuring Security and Trustworthiness

The process of user authentication is closely tied to system security. In a secure system, it is impossible to assume another user identity to gain access to (and potentially modify records in) the system. Not all records demand the same level of security. Alterations to an online staff phone directory will likely have significantly less risk than changes to the accounting records.

An ERS must protect records against change over time, either through unintended side-effects of software or through unauthorized access to the system. Other security considerations include user behaviors, including unsecured work stations, shared or easy-to-hack passwords, and social engineering hacks.

Specific requirements for general system security and trustworthiness should include the following.

› Determine appropriate levels of security based on risk and legal requirements, and select an appropriate authentication protocol (e.g., shared secret, PIN, or biometrics) and secure method of transmission during data entry or submission (e.g., PKI).[x]

› Limit system access (physical or via a network) to authorized individuals for specific purposes through appropriate security controls.[y] Physical security considerations include access to servers, unattended workstations, network wiring, remote access at the operating system or application level, and backup media. In general, access should be based on the principle of least privilege, granting users the minimum permissions necessary to perform their official duties.

› Ensure only authorized users can create records.[z] An ERS must include a current list of valid users with associated permissions to read, create, modify, or delete records, as well as contextual information on the authorization and de-authorization of users. Agency policies and procedures must include actions to be taken when a change in a user's status (hired, fired, changed position) affects access to the system. Users must not be authorized without proper documentation.

› An ERS must produce consistent results for the records it creates and must produce identical outcomes for all processes.[aa] In order to ensure that the electronic records system is the product of a consistent and credible set of processes, agencies must present evidence that the system is compliant with ANSI/AIIM Standard TR31-1994 "Performance Guidelines for the Legal Acceptance of Records Produced by Information Technology Standards." Systems should also be tested periodically to ensure compliance.

› Because an ERS is ultimately human-based, it is essential that the individuals who use and manage the system receive adequate training in all aspects of the system.[bb]

› The ERS should maintain an audit trail of system activity by system or application processes, and by user activity.[cc]

For more information see

› *Practical Tools for Electronic Records Management and Preservation*. Center for Technology in Government, SUNY. http://www.ctg.albany.edu/resources/pdfrpwp/mfa_toolkit.pdf.

Access Requirements[dd]

By law, "Public records and other matters in the custody of any officer shall be open to inspection by any person at all times during office hours" (ARS §39-121). Virtually all documents in the possession or control of a public officer are considered public records.[21]

An agency may refuse access if the record is made confidential by statute,[22] if the record involves the privacy interests of persons,[23] or disclosure would be detrimental to the best interests of the state.[24] More than 300 Arizona statutes address confidential records. A complete list may be found in the Arizona Attorney General's *Agency Handbook*.[25]

If an agency refuses an individual access to records on grounds of personal privacy or the best interests of the state, the individual may petition a court to review that decision. The court will make a decision within thirty days, and in most instances the courts have granted the individual access to the records. If an agency believes that records not specifically closed by law should not be made generally accessible to the public, it should develop a policy for denying access to or redacting those records. Having a policy in place ensures that decisions to deny access are well-reasoned and defensible, and avoids any appearance that the denial is to a specific individual.

› The general public must have access to the records. However, all users must follow authorization policies and procedures to access the ERS.[ee]

› An ERS must provide adequate search and retrieval capabilities to ensure that e-records can be retrieved for all legitimate business purposes throughout their full retention period.[ff] The ERS should be able to locate likely records using 'fuzzy logic' when search criteria are incomplete or imprecise. For example, it should be possible to locate records if a name is misspelled or only part of a name is name is known.

---

21 See Carlson, 141 Ariz. at 490, 687 P.2d at 1245. Quoted from Arizona Attorney General, *Agency Handbook*, chapter 6.

22 Berry v. State, 145 Ariz. 12, 13, 699 P.2d 387, 388 (Ct. App. 1985).

23 Scottsdale Unified School Dist. No. 48 v. KPNX Broad. Co., 191 Ariz. 297, 955 P.2d 534, 537 (1998).

24 Board of Regents v. Phoenix Newspapers, Inc., 167 Ariz. 254, 258, 806 P.2d 348, 351 (1991); KPNX-TV, 183 Ariz. at 592, 905 P.2d at 601.

25 Available online at http://www.attorney_general.state.az.us/Agency_Handbook/CHAPTER%206.pdf.

- An ERS should organize the records in a meaningful order to allow for browsing. Browsing many individual records can enable a user to discover patterns or information that cannot be formulated in a query.[gg]
- An ERS must be able to produce authentic copies of records and supply them in whatever form the user prefers.[hh]
- The agency must develop policies and procedures, some of which would be implemented in the ERS, to protect confidential or private information based on user permissions.[ii] An ERS must be able to redact confidential or private information.
- Arizona statute requires that the state be paid for commercial use of records. The agency should establish policies and procedures to ensure that it is compensated for commercial use of records.

Maintenance and Preservation Requirements

Manual recordkeeping systems require very little to ensure that they remain useful over time. Records created on paper today can be stored for decades then read, provided they have not been attacked by pest, fire, or flood.

Rapid changes in software and hardware make it highly unlikely that an electronic record created today could be read after twenty years. Many common office applications (word processors, spreadsheets) cannot read previous versions that are more than three generations old. Magnetic media is notoriously unstable and data suffers degradation within ten years; CD-RW is estimated to have an effective life of under twenty years. Even if the software can read an old file, there is a good chance that the hardware will not be available; try to find a player for a Beta tape or a 5.25" floppy drive.

To counter these problems agencies must plan to refresh and migrate their e-records. Agencies must also begin to account for these costs in their budgets. These costs are new to agencies, in that it was not necessary to duplicate paper records every five to ten years to ensure that they remain readable.

At some point all software packages will become obsolete, and routine migration will no longer suffice. Successful ERS design must assume and plan for major software or hardware changes by including a mechanism to communicate data from one system to a future system. Because it is impossible to know the nature of a future system, an ERS should be able to export records in a common data format that is well documented. Building this export function during the design phase significantly reduces migration costs because the individuals developing the function are intimately familiar with the ERS software and data storage methods. For more information on best practices for exporting data to neutral formats see [to be written].

In particular, digitally signed e-records must incorporate a mechanism to provide adequate validation of the signature over time. Agencies must determine how long it is necessary to authenticate signatures and must establish procedures to verify records that were authenticated by a service that is no longer available.

- The content, context, and structure of e-records must be preserved over the life of the record.[jj] Electronic records created in an ERS must be inviolate, in that they are not damaged, destroyed, or modified; coherent, in that when reconstructed, they represent the logical relations established by the original software environment (and not any updated platform or environment); and auditable, in that all actions taken to a record during the course of its life are documented with a proper audit trail.
- Develop retention solutions that are technologically neutral and that balance requirements for use, retention, human intervention, preservation, and security/encryption.[kk] Solutions should consider the length of time the records must be kept (short-term or long-term, but see below for permanent records), the necessary functionality of the original system, and the need to preserve the context and structure of the records.[ll] Solutions should require minimal human intervention.[mm]

- Establish preferred, standard file formats for data.[nn] Document non-standard file formats.
- Maintain records in encrypted form only as long as security warrants.[oo]
- An ERS must be able to export (migrate) records, including their content, context, and structure, to other systems without the loss of information.[pp]
- Agencies should refresh offline data on a routine basis to prevent bit loss or other problems associated with the physical degradation of media.
- Agencies should develop business continuity and disaster recovery policies and procedures.[qq] Such policies and procedures should address routine data backup, verification of backups, offsite storage of data, and proper labeling of media.
- Agencies should ensure that backup media are overwritten or destroyed in a timely manner so that any obsolete records deleted from the system are not keep significantly longer than the scheduled retention period. Copies of records on backup media are discoverable, even if the record copy has been deleted from the system. A discovery order could require an agency to search through all extant backup media for relevant records.

For more information on best practices for managing digital signatures see . . . .

Disposal: Archival Storage and Destruction

- Retain records in accessible form for their legal, minimum retention periods as established by Records Management Division.[rr]
- An ERS must be able to delete records.[ss] However, an ERS must be able to protect selected records from routine destruction.
- Records that may be relevant to pending litigation must not be destroyed, even if those records have passed their retention period.
- Records scheduled for permanent retention must be exported to permanent media as defined by Arizona statute.[tt] Note that the original electronic copies need not be destroyed when the archival copy is created.
- Sufficiency of disposal/thoroughness of destruction (deletion, erasure, physical destruction of media).

APPENDIX A. ARCHIVAL APPRAISAL CRITERIA

The Arizona State Archives identifies, collects, preserves, and provides access to records in all formats of Arizona state and local governments and of public officials and other individuals. Archival records remain useful for the Legislature, state agencies, and the general public because those records make government accountable to its citizens; provide evidence about public policies and programs; and protect or verify individuals' rights and entitlements. Archival records provide information about the important people, issues, places, and events that make up the story of Arizona's history.

ARCHIVAL VALUE

The Arizona State Archives is legally mandated to collect and preserve the history of Arizona and its government. The number of archival records is very small, typically two to five percent of the whole of an agency's records.

State Archives and Records Management Division staff work with state agencies and local governments to identify those records with sufficient value to warrant the resources necessary to preserve them in perpetuity and document those appraisal decisions on a records retention schedule. Archivists use their knowledge of Arizona history and their familiarity with other records in the Archives when appraising records. They look for records that add to, complement, or fill gaps in the existing records that document Arizona history.

Archivists use the following criteria in combination to distinguish those records which have lasting value.

- Users
- Creator/Office of Origin
- Evidence of Programs or Functions (Functional Value)
- Content (Informational Value)
- Preservation of Individuals' Rights and Entitlements
- Completeness
- Relationship to Other Records
- Age of the Records
- Format

Agency staff who have questions about which records are archival should flag such records for review by the Archives before they are destroyed, even if the destruction is authorized on a retention schedule.

USERS

The Archives collects records that retain value for its users, the Legislature, state and local agencies, and the general public. The Archives looks for types of records that are supported by existing patterns of use.

CREATOR / OFFICE OF ORIGIN

The Archives collects the records of state and local government in Arizona. Every agency, large and small, creates records which document policies and programs, and those records are valuable to the Archives.

In addition to public records, the Archives also collects the personal papers of public officials and of other individuals or groups if they contain significant information relating to Arizona government, public policies and programs, or the history of Arizona.

To ensure that archival records are authentic and reliable, the content of the records should not have deteriorated through fraudulent change or loss. Changes made by the record creator (or the creator's agent) should be documented so that such changes are readily apparent. Note, however, that there is no requirement that records be accurate; in some instances, it is important to preserve inaccurate records to document that information used to make decisions or to prove fraud.

Records of questionable origin are of questionable archival value. The Archives seeks to collect the original records of the agency which created them or its successor; it generally does not collect copies of an agency's records held by another agency.

Simple association with a notable individual – a mention, a signature – does not, alone, make a record archival.

EVIDENCE OF PROGRAMS OR FUNCTIONS (FUNCTIONAL VALUE)

Records which document the principal responsibilities of the agency or office and that explain programs that help agencies accomplish their missions by documenting the decision making process are likely to be archival. In particular, the Archives seeks to acquire and preserve those records that document the agency's organization, that provide continuity between changes in office, and that demonstrate government accountability.

Administrative records relating to an agency's day-to-day operations are generally not preserved in the Archives. These records include general memoranda, human resources files, facilities files, routine activity reports, and similar records.

Because agencies' policies and programs affect constituents, correspondence and other records documenting public concerns and opinions regarding controversial or divisive policies or programs often warrant archival preservation.

CONTENT (INFORMATIONAL VALUE)

Some records retain their value over time because they contain information about topics that help define the history and character of the state. Records relating to water, agriculture, mining, tourism, urban growth, environmental quality, multiculturalism, and the economy – among other topics – will continue to have archival value. As time passes, new topics will take on archival value.

Records that provide substantial, unique information and background relating to a newsworthy event are often candidates for the Archives.

PRESERVATION OF INDIVIDUALS' RIGHTS AND ENTITLEMENTS

The Archives collects many records that document individuals' enduring rights or benefits under government programs. Examples include, but are not limited to, rights of citizenship, civil status (birth, death, marriage, and divorce), and ownership of real property. The Archives generally does not collect records that detail temporary benefits individuals have received from government programs, such as welfare or public health.

COMPLETENESS

The Archives typically collects an entire record series rather than trying to identify individual files of historical value. (A record series is a group of identical or related records which are normally used and filed as a unit).

In rare circumstances, the Archives may collect sample records from a large series of limited value to document a process or function performed by the agency. Neither the frequency of use nor the size of an individual file necessarily indicate archival value, but use and size may serve as useful flags for more careful appraisal.

RELATIONSHIP TO OTHER RECORDS

The Archives prefers to collect originals, rather than copies, because it is easier to demonstrate the authenticity and reliability of original records.

Records that contain detailed information may be added to the Archives, in addition to summary reports, if other methods of analysis may yield findings significantly different from those in the summary.

A record series is generally not acquired for the Archives if the information contained in those records is routinely repeated in another series that the Archives already collects.

FORMAT

The Archives collects records in all formats, including – but not limited to – papers, photographs, and video and audio recordings. The Archives also collects text, images, and sounds in electronic format.

Format occasionally makes records more valuable because it increases their usefulness. A record series in paper may not be collected in paper format because analysis is impractical. However, that series might be collected if it is in electronic format because use of a computer makes complex analysis practical.

AGE OF THE RECORDS

Archives are not collections of nostalgia and historical curiosities. Age alone does not justify preservation.

The Archives seeks to evaluate all records from the Territorial Period before disposal. These records were often labeled with terms that today would suggest the records are not archival. Closer examination of those records' content may reveal that the description is inaccurate and that the records should be retained permanently.

ISSUES TO ADDRESS

Do the guidelines emphasize sufficient audit trails? For example, general ledgers may not be sufficient; auditors want to know the details of how the information in the general ledgers was created to ensure that the underlying data is correct.

Capture of records created by contractors (other third parties) outside normal systems. (Jill Harvey)

Many legacy ERS were designed as systems to create records and lack important records management functions. In particular, they often cannot schedule records for disposal. Many lack the ability to export data to facilitate system migration. The State of Delaware surveyed ERS used by state agencies and discovered that many legacy ERS met most recordkeeping requirements, although a few systems lack critical functions. Arizona agencies should evaluate their legacy systems using the requirements outlined in this document to determine what functionality should be added to the system. As with all records management, the costs of implementing that functionality should be weighed against the benefits; for example, it makes no sense to invest in a system that contains records of limited value is to be decommissioned in short order.

Mention role of federal agencies in recordkeeping?

Most of the general requirements for recordkeeping is introductory material, not requirements. This section should describe essential characteristics of records and recordkeeping systems (as distinct from information/systems). E.g., content, context, structure; immutability; extrinsic and intrinsic elements; essential elements (author, date, subject, etc.); metadata necessary to replicate the characteristics of paper records.

EQUIVALENCIES IN NECCC AND DELAWARE ERS GUIDELINES

NECCC: National Electronic Commerce Coordinating Committee, *Electronic Records Management Guidelines for State Governments*.

D: Delaware Public Archives. *Model Guidelines for Electronic Records* (http://www.state.de.us/sos/dpa/govserv/records%20policies/2model%20guidelines.htm).

a	NECCC 1.3:91-98, NECCC 2.1.1:124
b	NECCC 1.2:67-90
c	NECCC 1.1:14
d	D2.C.2
e	NECCC 2.2:133, 4:423
f	NECCC 2.1.1:124
g	NECCC 3.1.1:214, 4.1.1:435, D2
h	NECCC 4.1:476, 4.1.3:460, 4.1.4:477, 4.2.2:503, 4.1.2:435
i	NECCC 1.1:49, D1
j	NECCC 2.1:120, 3.1:211, D7, D9
k	NECCC 4.1.5:488
l	NECCC 4.1, D2
m	NECCC 4.1.2: 455
n	NECCC 4.1.3: 460
o	NECCC 4.1:476, 4.1.3:460, 4.1.4:477, 4.2.2:503, 4.1.2:435
p	NECCC 4.1.5: 488
q	NECCC 2.1.1:124
r	NECCC 2.1:120
s	NECCC 2.2.4:175
t	NECCC 2.3:191
u	NECCC 3.2
v	NECCC 2.1.3:129
w	NECCC 2.2.5:183
x	NECCC 2.2:143, 2.3: 166
y	NECCC 4.3:520
z	NECCC 2.3:166, NECCC 4.3:520, D8
aa	NECCC 4.1:432, 4.2.2:503, D4
bb	NECCC 4.1.5:488
cc	NECCC 4.1.4: 477
dd	NECCC 3.3:350, 3.4:358
ee	NECCC 3.4.4:415
ff	NECCC 3.3.1:353
gg	NECCC 3.1.2:245
hh	NECCC 3.4:358, NECCC 3.4.4:415
ii	NECCC 3.4.1:362, 3.4.2:366, 4.3:520, D13
jj	D9
kk	NECCC 3.2:253, 3.2.4:304
ll	NECCC 3.3: 280ff
mm	NECCC 3.4:300
nn	NECCC 3.1.1.2:228, 3.2.1:265, 3.2.7:325
oo	NECCC 3.2.2
pp	NECCC 3.7:318, D11, D12

[qq] NECCC 4.2:495, 4.2.1:498, 4.2.3:514
[rr] NECCC 3.2:253
[ss] D10
[tt] NECCC 3.2.1:265, 3.2.6:310, 3.2.7:337